プレスリリース
第 11-31-229 号
2011 年 9 月 5 日
独立行政法人情報処理推進機構

コンピュータウイルス・不正アクセスの届出状況［2011 年 8 月分］について

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、2011 年 8 月のコンピュータウイルス・不正アクセスの届出状況をまとめました。

1. 今月の呼びかけ

「 あなたの銀行口座も狙われている！？ 」
― SpyEye（スパイアイ）ウイルスに注意！ ―

2011 年 6 月から 7 月にかけて、インターネットバンキングでの不正利用事件が発生しています。警察に約 10 の金融機関から被害相談や届出が出されていると報道されるなど、事態の深刻さを受け、IPA でも 8 月に緊急対策情報※1 として注意喚起を行いました。

この不正利用事件は、「SpyEye（スパイアイ）」というウイルスの感染被害で起こった可能性が考えられます。それは、SpyEye ウイルスに、日本の銀行を不正利用する機能が含まれていたためです。

IPA では、SpyEye の一種（v1.3.45）を入手し、解析を実施中です。今のところ全ての解析を終えていませんが、ここでは、現時点で判明している解析結果を基に、SpyEye とはどのようなウイルスで、感染するとどのような動作をするのかを示すとともに、被害に遭わないための対策を紹介します。

※1 IPA-「国内のインターネットバンキングで不正アクセスが相次いでいる問題について」
http://www.ipa.go.jp/security/topics/alert20110803.html

（1）SpyEye とは？

SpyEye とは、本来ウイルスを作成するツールの名称ですが、このツールから作成されたウイルスも SpyEye と呼ばれるため、ここでは、作成されたウイルス自体を指すことにします。

SpyEye は、こうしたツールから簡単に作成することができ、また、少しずつ機能の異なる SpyEye を簡単に作成できるため、多くの亜種が存在しています。

図 1-1：ウイルス作成者がツールを使ってウイルスを作り出すイメージ図

【i】SpyEye の出現

SpyEye は、インターネットバンキングで使われる ID とパスワードの窃取を目的としたウイルスです。最初の出現は、2009 年の終わり頃から 2010 年初めにロシアのアンダーグラウンドサイト※2 からと言われています。

それまで、インターネットバンキングの ID とパスワードの窃取を目的としたウイルスは、Zeus（ゼウス）と呼ばれるウイルスを作成するツールから作成されたウイルス（Zeus、Zbot）が主立ったものでした。SpyEye は、この Zeus を基に作られたものと考えられています。

※2　アンダーグラウンドサイト：インターネットを通じて、違法行為や犯罪行為の勧誘や依頼を受けるウェブサイト。

【ii】感染後の動作

今回の解析から、SpyEye の感染後の動作として次の 2 点を確認しました。

- 利用者が閲覧中のウェブサイトで入力した ID とパスワードを窃取
- 窃取した情報をインターネット経由でウイルス作成者が管理しているサーバーに送信

SpyEye がパソコンに感染すると、利用者が閲覧しているインターネットバンキングなどのウェブページで ID とパスワードの情報を窃取し、インターネットを通じてボット※3 に感染したパソコンを操作する特定のサーバーに情報を送信します。これは、SpyEye がボットネット※4 機能を有していることを示しています。

ボットネット機能を使えば、ウイルス作成者がインターネットを通じて感染させた SpyEye を新しいウイルスに置き換えることができます。ウイルス対策ソフトで検知できない新種ウイルスに置き換え続けることで、より見つかりにくく、長い期間感染させて必要な情報を窃取できるため、利用者にとって重大な脅威となるウイルスといえます。

※3　ボット（bot）：ボットとはウイルスの一種で、ボットに感染したパソコンは、インターネットを通じて外部から操られてしまいます。

※4　ボットネット（botnet）：ボットネットとは、ボット（bot）に感染したパソコンとそれを操作するサーバーからなるネットワークのこと。

（ご参考）

ボット対策のしおり（IPA）

http://www.ipa.go.jp/security/antivirus/documents/3_bot_v6_2.pdf

（2）SpyEye の感染手口

SpyEye の主な感染手口として、次の 2 つが考えられます。

【i】ウェブサイトからダウンロードさせる

ウェブサイトを閲覧した際に、パソコン利用者の意図に関わらず、ウイルスなどの不正プログラムをパソコンにダウンロードさせる手法で「"ドライブ・バイ・ダウンロード"攻撃」と呼ばれます。"ドライブ・バイ・ダウンロード"攻撃では、主に利用者のパソコンの OS やアプリケーションなどの脆弱（ぜいじゃく）性が悪用されます。
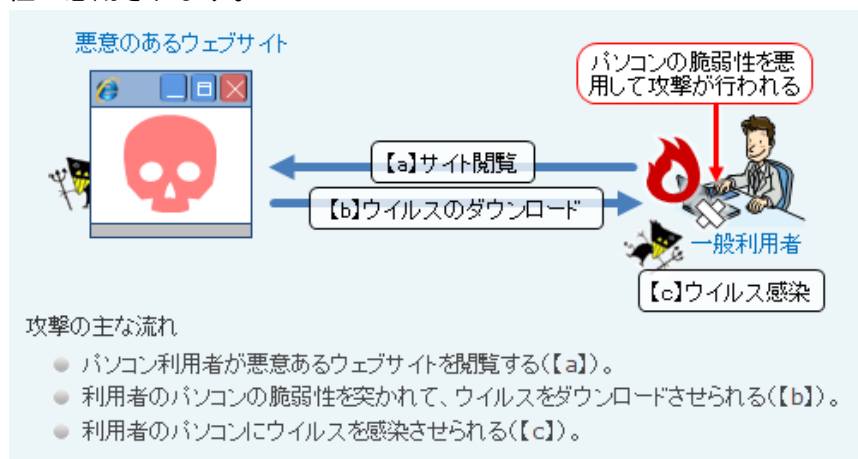
図 1-2："ドライブ・バイ・ダウンロード"攻撃のイメージ

ウイルスを感染させる際の常とう手段となっている”ドライブ・バイ・ダウンロード”攻撃ですが、SpyEye を感染させる手口にも使われています。

（ご参考）

「ウェブサイトを閲覧しただけでウイルスに感染させられる"ドライブ・バイ・ダウンロード"攻撃に注意しましょう！」（IPA）

http://www.ipa.go.jp/security/txt/2010/12outline.html

【ii】メールで送りつける

ウイルスが感染している添付ファイル付きメールを送り、添付ファイルを開かせて感染させる手口も既に常とう手段となっています。この手口では、タイトルや添付ファイル名、メール本文や送信元詐称などによって、なんとかしてメールの添付ファイルを開かせようとします。

最近では、関係機関や関係者を装い、組織や個人を絞ってウイルスが感染している添付ファイルを送りつける「標的型攻撃」メールも多くなっています。

（ご参考）

災害情報を装った日本語のウイルスメールについて（IPA）

http://www.ipa.go.jp/security/topics/alert20110404.html

（3）対策

【i】OS やアプリケーションソフトの脆弱性を解消する

Windows などの OS や、アプリケーションの脆弱性を解消しておくことが重要です。**一般的に利用者の多いアプリケーションは狙われやすい傾向にあるため、脆弱性を解消して、常に最新の状態で使用してください。IPA では利用者のパソコンにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツール「MyJVN バージョンチェッカ」を公開しています。なお、8 月 18 日から、サーバーに導入しているソフトウェアのバージョン確認や、Windows7（64bit 版）にも対応しました。**

（ご参考）

MyJVN バージョンチェッカ（IPA）

http://jvndb.jvn.jp/apis/myjvn/vccheck.html

サーバーソフトウェアもチェック可能となった「MyJVN バージョンチェッカ」

～システム管理者は脆弱（ぜいじゃく）性対策がなされたサーバーソフトウェアの使用を～

http://www.ipa.go.jp/about/press/20110818.html

【ii】ウイルス対策ソフトでウイルスの侵入を防止する

ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保つことで、ウイルスの侵入阻止や、侵入したウイルスの駆除ができます。**近年のウイルスは、パソコンの画面の見た目では感染していることが分からないものが多いため、ウイルスの発見と駆除にはウイルス対策ソフトが必須です。**

【iii】簡単にメールの添付ファイルを開かない

普段やり取りがない送信者からのメールが届いたら、不用意に開いたり、メール本文に書いてあるリンクを安易にクリックしたりしないでください。可能であれば送信者と連絡を取り、本当にその送信者が送ったメールなのかを確認してください。ただし、確認をする際は、メールの中に書かれている連絡先には連絡をせず、出来る限り自分で連絡先を調べて電話で確認することを勧めます。

添付ファイルがあるメールであれば、普段やり取りのある送信者からのメールでも用心し、少しでも不自然だと思うメールであれば、相手に確認を取るか、メールそのものを読まずに削除することが最善策です。

【iv】ID やパスワードを使い回さない

SpyEye は、インターネットバンキングで使われる ID とパスワードの窃取を目的としています。**もし、感染被害に遭い ID とパスワードを窃取されてしまった場合、その ID やパスワードを他のウェブサイトでも使い回していると、そのウェブサイトのサービスでも連鎖的に不正利用の被害に遭う可能性があります。**

パスワードは、いつでも悪意ある者に狙われているという意識を持つべきです。また、下記のウェブページを参考にしてパスワードの適切な管理を心がけてください。

インターネットバンキングでは、その時だけ有効なパスワードを発行する「ワンタイムパスワード」というサービスを提供していることがあります。ID やパスワードを盗むウイルスに感染していても、一度きりのパスワードのため、仮に盗まれてもその後悪用されることはありませんので、このサービスの利用をお勧めします。

（ご参考）

「パスワード ぼくだけ知ってる たからもの」（IPA）

http://www.ipa.go.jp/security/txt/2011/06outline.html

【v】ウイルスに感染してしまった場合の対策

SpyEye に限らず、ウイルスに感染した疑いがある場合（動作が遅い、不自然な動きをする、出所不明なファイルを開いてしまったなど）は、まず、ウイルス定義ファイルが最新の状態になったウイルス対策ソフトで、パソコン内のウイルスチェックを行ってください。

SpyEye は、ウイルス作成者がいつでも新しい SpyEye に置き換えることができるため、ウイルス対策ソフトで発見されない場合があります。ウイルスチェックをしても見つからない、または駆除をしたにもかかわらず正常に動作していないと思われるのであれば、パソコンを購入した時の状態に戻す作業（初期化）を行ってください。

実際の作業方法は、パソコンに付属の取扱説明書に記載されている「購入時の状態に戻す」などの手順に沿って作業してください。なお、作業を行う前には、重要なデータのバックアップを忘れずに行ってください。また、バックアップしたデータは、パソコンに戻す前にウイルス対策ソフトでウイルスチェックし、ウイルスが含まれていないことを確認してください。

もし、インターネットバンキングの不正利用の被害に遭ってしまった場合は、当該銀行への問い合わせをしてください。多くの銀行では、ウェブサイトのトップページから問い合わせができるようになっています。さらに、ウイルスに感染していない、自分自身が管理している安全なパソコンから、インターネットバンキングで使用しているパスワードを変更してください。

今月のトピックス

○ コンピュータ不正アクセス被害の主な事例（届出状況および被害事例の詳細は、7 頁の「3.コンピュータ不正アクセス届出状況」を参照）
- サーバーに不正にログインされ、ファイルを置かれた
- SQL インジェクション攻撃でクレジットカード情報が盗まれ、不正使用された

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、9 頁の「4.相談受付状況」を参照）
- 無料だと思い、パソコンの処理速度を向上するソフトをインストールしてみた
- Twitter アカウントをなりすまされている

○ インターネット定点観測（11 頁参照。詳細は、別紙 3 を参照）

IPA で行っているインターネット定点観測について、詳細な解説を行っています。

2. コンピュータウイルス届出状況　－詳細は別紙 1 を参照－

（1）ウイルス届出状況

8 月のウイルスの検出数※1 は、**約 2.5 万個**と、7 月の約 2.3 万個から 9.6%の増加となりました。また、8 月の届出件数※2 は、**931 件**となり、7 月の 1,064 件から 12.5%の減少となりました。

※1 検出数　：届出にあたり届出者から寄せられたウイルスの発見数（個数）
※2 届出件数：同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何個検出されても届出 1 件としてカウントしたもの。

・8 月は、寄せられたウイルス検出数約 2.5 万個を集約した結果、931 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 1.4 万個**、2 位は **W32/Mydoom** で**約 9.0 千個**、3 位は **W32/Autorun** で**約 0.6 千個**でした。

図 2-1：ウイルス検出数

ウイルス届出件数 931件（1,064件）前月比　－12.5%
（注：括弧内は前月の数値）
その他 200件 21.5%（220件 20.7%）
Mytob 50件 5.4%（63件 5.9%）
Bagle 63件 6.8%（31件 2.9%）
Downad 69件 7.4%（70件 6.6%）
Mydoom 200件 21.5%（231件 21.7%）
Netsky 196件 21.1%（236件 22.2%）
Autorun 153件 16.4%（180件 16.9%）
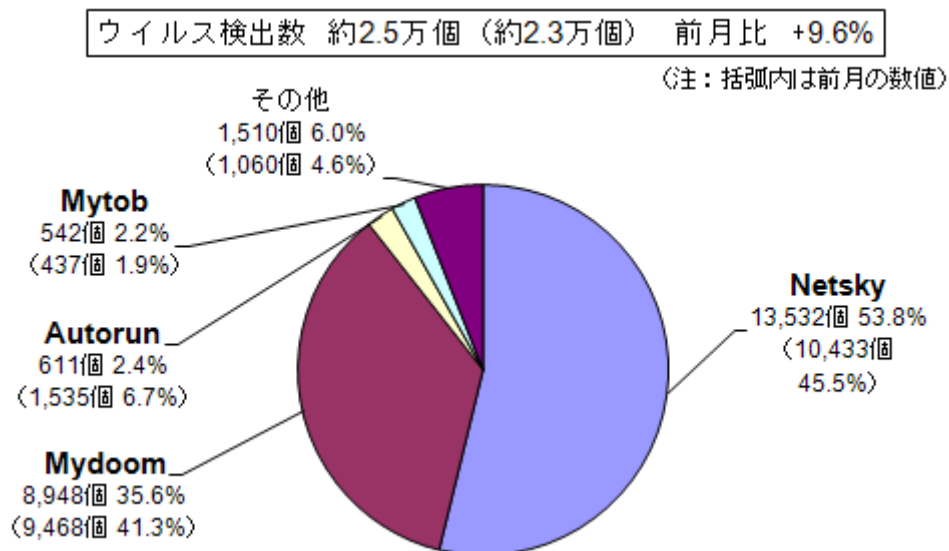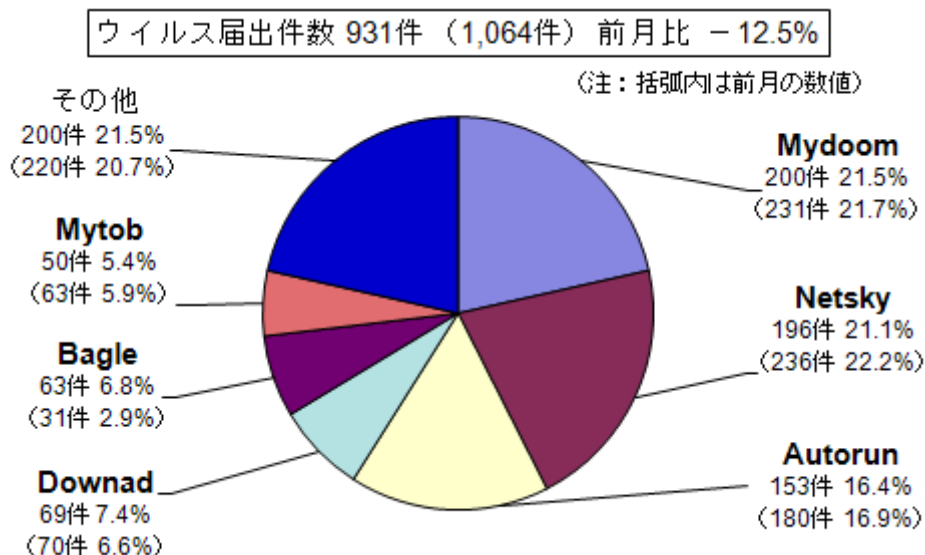
図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

8 月は、別のウイルスを感染させようとする DOWNLOADER といった不正プログラムが増加傾向となりました（図 2-3 参照)。
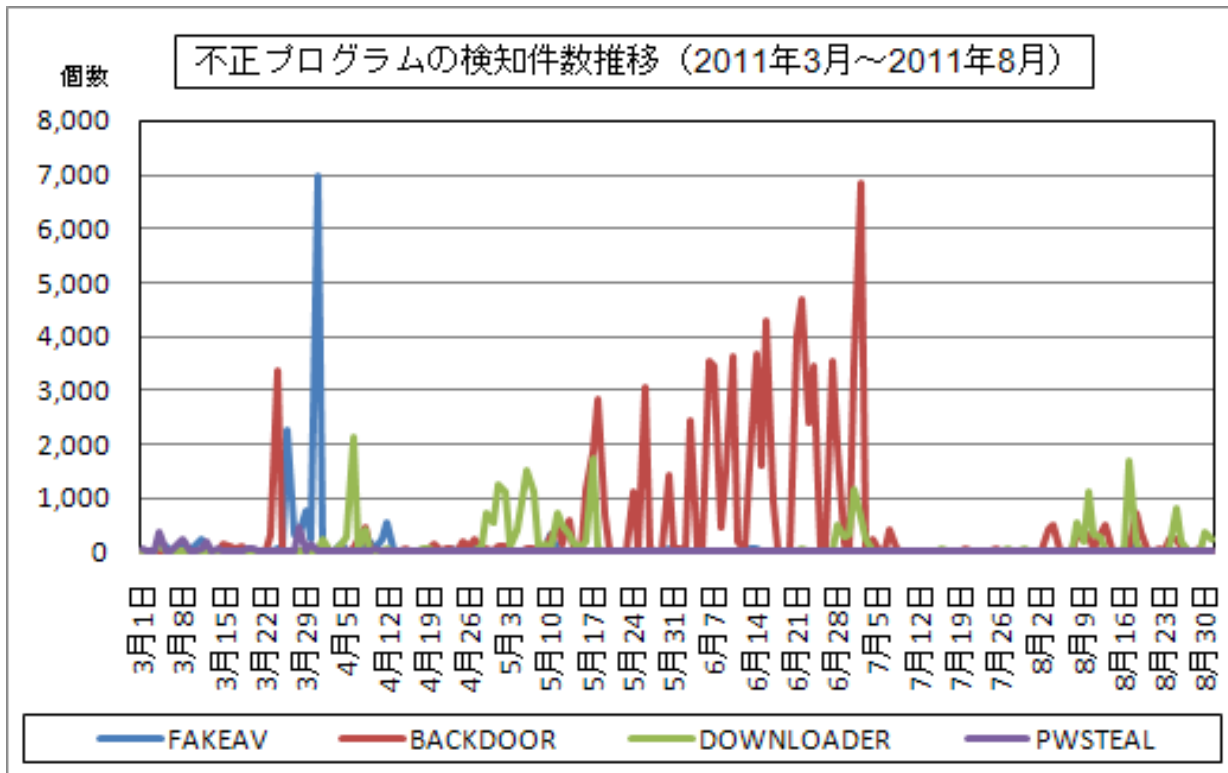
図 2-3：不正プログラムの検知件数推移

9 月から 12 月の期間は、正規のウイルス対策ソフトの最新版が発表される時期となりますが、これに乗じて、「偽セキュリティ対策ソフト」型ウイルスを筆頭に不正プログラムが増加すると考えられます。

利用者は、以下のウェブページを参考にして、感染被害に遭わないように対策を施してください。

（ご参考）

「深刻化する偽セキュリティ対策ソフトの被害！」（IPA）

http://www.ipa.go.jp/security/txt/2010/06outline.html

3. コンピュータ不正アクセス届出状況（相談を含む）　－詳細は別紙 2 を参照－

表 3-1　不正アクセスの届出および相談の受付状況

		3月	4月	5月	6月	7月	8月
届出[(a)] 計		6	5	7	9	8	10
	被害あり[(b)]	6	5	6	9	5	8
	被害なし[(c)]	0	0	1	0	3	2
相談[(d)] 計		45	38	55	32	47	37
	被害あり[(e)]	10	10	14	7	15	13
	被害なし[(f)]	35	28	41	25	32	24
合計[(a+d)]		51	43	62	41	55	47
	被害あり[(b+e)]	16	15	20	16	20	21
	被害なし[(c+f)]	35	28	42	25	35	26

（1）不正アクセス届出状況

8 月の届出件数は 10 件であり、そのうち何らかの被害のあったものは 8 件でした。

（2）不正アクセス等の相談受付状況

不正アクセスに関連した相談件数は 37 件であり､そのうち何らかの被害のあった件数は 13 件でした。

（3）被害状況

被害届出の内訳は、**侵入 7 件、DoS 攻撃 1 件**でした。

「侵入」の被害は、メールアカウントを外部から勝手に使われて迷惑メール送信に悪用されていたものが 1 件、ウェブページが改ざんされていたものが 1 件、データベースからクレジットカード情報が盗まれたものが 1 件、外部サイトを攻撃するツールを埋め込まれ、踏み台として悪用されていたものが 3 件、でした（他は詳細不明）。侵入の原因は、ファイアウォールの設定不備が 1 件、ID やパスワード管理不備と思われるものが 1 件、ウェブアプリケーションの脆弱性を突かれたものが 1 件でした（他は原因不明）。

（4）被害事例

［侵入］

(i）サーバーに不正にログインされ、ファイルを置かれた

事例	・サーバーのメンテナンス中に、見知らぬプログラムが実行されているのを発見。 ・root 権限は奪われていなかったが、既存の一般ユーザーで不正にログインされた後に 2 種の不正プログラムを埋め込まれ、外部サイト攻撃の踏み台として使われていた。 ・埋め込まれていた不正プログラムは、IRC ボットおよび外部サイトへの DoS 攻撃ツール、であった。即刻それらのプログラムを停止し削除した。その後、該当ユーザーのディレクトリとアカウントを削除した。 ・事後対策として、不要な休眠アカウントの削除と、全ユーザーのパスワード変更を実施した。
解説・対策	サーバーに埋め込まれていた不正プログラムが何だったのか明らかにされた、貴重な例です。明らかに、悪意ある者が当該サーバーを操作し、他のサーバーを攻撃しようとしていたことが伺えます。このように、セキュリティの弱いサーバーは、他のサイトを攻撃するための**踏み台として乗っ取られるかも知れないという脅威に常に晒されています**。管理や設定の抜けが無いか、今一度、確認してください。 （参考） IPA - ボット対策について http://www.ipa.go.jp/security/antivirus/bot.html

(ii）SQL インジェクション攻撃でクレジットカード情報が盗まれ、不正使用された

事例	・オンラインショッピングサイトを運営している。クレジットカード会社から、カード不正利用に関する照会があった。 ・調査の結果、外部からの SQL インジェクション攻撃が成功していた。また、本来存在しないはずのクレジットカード情報がデータベースに残っていて、その情報を攻撃者によって抜き取られてしまったことが判明。 ・事後対策として、クレジットカード決済を自社ウェブサイト上ではなく、決済代行会社のウェブサイト上で行うように変更する予定。また SQL インジェクション対策としてソースコードレビューを行う予定。
解説・対策	不要なデータが残ったままになっていたことが、情報漏えいにつながってしまった残念な例です。不要なテーブルやデータを定期的に削除することは、データベースの肥大化やパフォーマンス低下を抑えるために有効ですが、情報漏えい防止の観点からも実施することを勧めます。 金銭の決済をするサイトでは、一度事故が発生するとその被害は甚大となります。サイト運用の際には、**侵入検知システム（IDS/IPS など）や WAF を導入**し常に監視の目を光らせるとともに、定期的に、**専門業者にウェブサイトの脆弱性検査を依頼**することを勧めます。本事例のように、**決済業務を外部委託**することも有効です。 （参考） IPA - ウェブサイト運営者のための脆弱性対応ガイド http://www.ipa.go.jp/security/fy19/reports/vuln_handling/ IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

4. 相談受付状況

8 月のウイルス・不正アクセス関連相談総件数は **1,651 件**でした。そのうち**『ワンクリック請求』に関する相談**が **535 件**（7 月：461 件）、**『偽セキュリティソフト』**に関する相談が **7 件**（7 月：8 件）、**Winny に関連する相談**が **7 件**（7 月：7 件）、**「情報詐取を目的として特定の組織に送られる不審なメール」に関する相談**が **0 件**（7 月：2 件）、などでした。

表 4-1　IPA で受け付けた全てのウイルス・不正アクセス関連相談件数の推移

		3月	4月	5月	6月	7月	8月
合計		1,723	1,608	1,640	1,692	1,490	1,651
	自動応答システム	1,106	997	950	999	889	958
	電話	551	555	620	639	540	639
	電子メール	58	50	62	50	54	50
	その他	8	6	8	4	7	4

※ IPA では、「情報セキュリティ安心相談窓口」を開設し、コンピュータウイルス・不正アクセス、Winny 関連、その他情報セキュリティ全般についての相談を受け付けています。
メール：anshin@ipa.go.jp
電話番号：03-5978-7509　（24 時間自動応答、ただし IPA セキュリティセンター員による相談受付は休日を除く月～金の 10:00～12:00、13:30～17:00 のみ）
FAX：03-5978-7518　（24 時間受付）

※ 「自動応答システム」：電話の自動音声による応対件数
「電話」：IPA セキュリティセンター員による応対件数

※ 合計件数には、「不正アクセスの届出および相談の受付状況」における『相談（d）計』件数を内数として含みます。
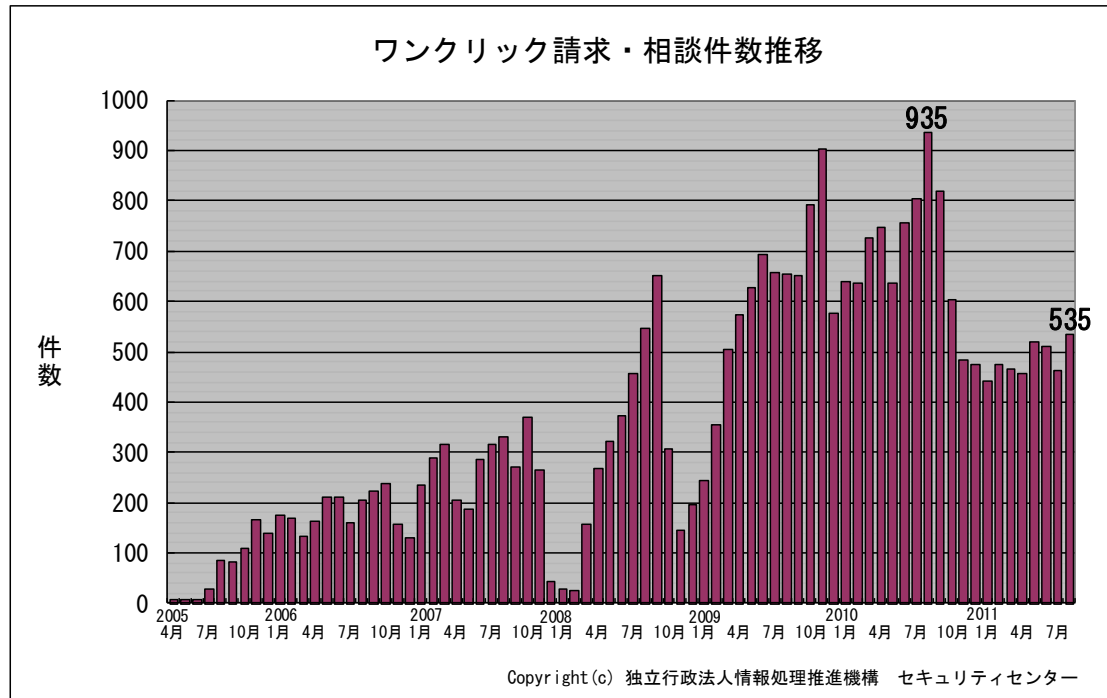
図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）無料だと思い、パソコンの処理速度を向上するソフトをインストールしてみた

相談	何気なくウェブサイトを見ていた時に、「パソコンの処理速度を向上。まずは無料ソフトでエラーチェックを。」といった広告を見つけた。特に警戒もせずにクリックして先に進み、ソフトをインストールして実行したところ、たちまち大量のエラーが検出され、修復するためには有料版ソフトの購入が必要だと警告してきた。 無料ならということで試しただけなので購入するつもりもないが、インストールしてしまったソフトをどうやって削除したらいいか分からなくて困っている。
回答	一般的なアプリケーション（プログラム）であれば、Windows Vista/7 の場合は、「コントロールパネル」の「プログラムのアンインストール」から、Windows XP の場合は、「コントロールパネル」の「プログラムの追加と削除」から、該当すると思われるプログラム名を「アンインストール」または「削除」することで削除できるはずです。 ウェブサイトを見ていると、こういったパソコン利用者の興味を引く広告を目にすることがありますが、**出所の分からないソフトは利用するべきではありません**。ソフトの選定に自信が無い場合は、ウェブサイトからのダウンロード販売による購入は避け、パソコンショップなどの店頭で店員の説明を聞くなどしてからの購入を勧めます。

（ii）Twitter アカウントをなりすまされている

相談	自分で登録した Twitter アカウントが、第三者にパスワードを破られて、乗っ取られてしまった。そのアカウントから、本人（私）になりすまして、自らの評判を落とすような内容のツイートを書き込むといった悪質な行為が行われている。 なんとかして悪質な書き込みをやめさせたいが、どうしたらいいか分からない。
回答	Twitter のアカウントを乗っ取られると、本人が書いたように見せかけて、第三者が自由に書き込みを行えるため、非常に厄介です。 この場合、**早急になりすましの事実を Twitter 側に報告し、当該アカウントの削除などを依頼してアカウントを停止することが先決です**。また、必要に応じて警察に被害届けを出すことも検討してください。 Twitter 社ではこのような被害を想定して、ヘルプセンターのページを設けていますので、以下のページの「規約違反の報告について」の項目を参考にして、なりすましの事実を報告することをお勧めします。 また、再び同じ被害に遭わないために、パスワードのセキュリティ対策を一度見直してみることをお勧めします。 （ご参考） Twitter ヘルプセンター http://support.twitter.com IPA-2010 年 5 月の呼びかけ「 パスワード ぼくだけ知ってる たからもの 」 http://www.ipa.go.jp/security/txt/2011/06outline.html

5. インターネット定点観測での 8 月のアクセス状況

インターネット定点観測（TALOT2）によると、2011 年 8 月の期待しない（一方的な）アクセスの総数は 10 観測点で **106,910 件**、延べ発信元数※は **46,101 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 149 の発信元から 345 件のアクセスがあった**ことになります（図 5-1 参照）。

延べ発信元数※：TALOT2 の各観測点にアクセスしてきた発信元を単純に足した数のことを、便宜上、延べ発信元数とする。ただし、同一発信元から同一の観測日・観測点・ポートに複数アクセスがあった場合は、発信元数を 1 としてカウントする。

TALOT2 における各観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。
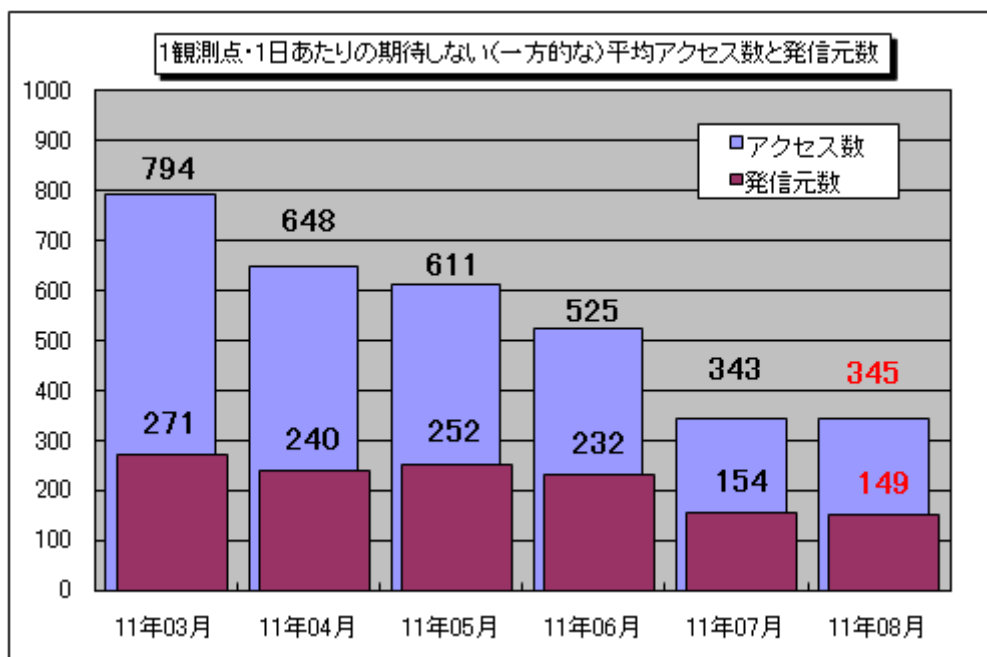
図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

上記グラフは 2011 年 3 月～2011 年 8 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を示しています。8 月の期待しない（一方的な）アクセスは、7 月と比べてほぼ同程度でした。

7 月と 8 月の宛先（ポート種類）別アクセス数の比較を図 5-2 に示します。7 月に比べ、増加が観測されたのは、22936/udp、10394/udp、および 3389/tcp へのアクセスでした。

22936/udp、および 10394/udp はいずれも、特定のアプリケーションで使用されるポートというわけではなく、これらのアクセスが何を目的としたものだったかは不明ですが、どちらも特定の 1 観測点のみで観測されていました。

3389/tcp は、8 月の後半に増加が観測されており（図 5-3 参照）、国内で定点観測を行っている他の組織でもほぼ同様の傾向が観測されていたとのことです。このポートは、主に RDP※1 で使用されるポートであり、このポートを悪用して Windows 端末に感染を広げる「Morto※2」と呼ばれるウイルスが見つかっているため、このアクセスがウイルスの感染活動によるものだった可能性があります。

Windows 上でリモートデスクトップなどの機能を使用している方は、ウイルスの感染被害に遭わないために、ウイルス対策を再確認するとともに、ログインの際のパスワードを強化するなどの対策を行ってください。

※1 RDP（Remote Desktop Protocol）：遠隔で Windows 端末の操作ができるリモートデスクトップ機能などで使われるプロトコルのこと。

※2 Morto：RDP を悪用して Windows 端末に感染するウイルスの一種。感染すると 3389/tcp にポートスキャンを行いリ

モートデスクトップ機能が有効な端末を探索し、発見した端末に対してパスワードクラッキングを試みる。
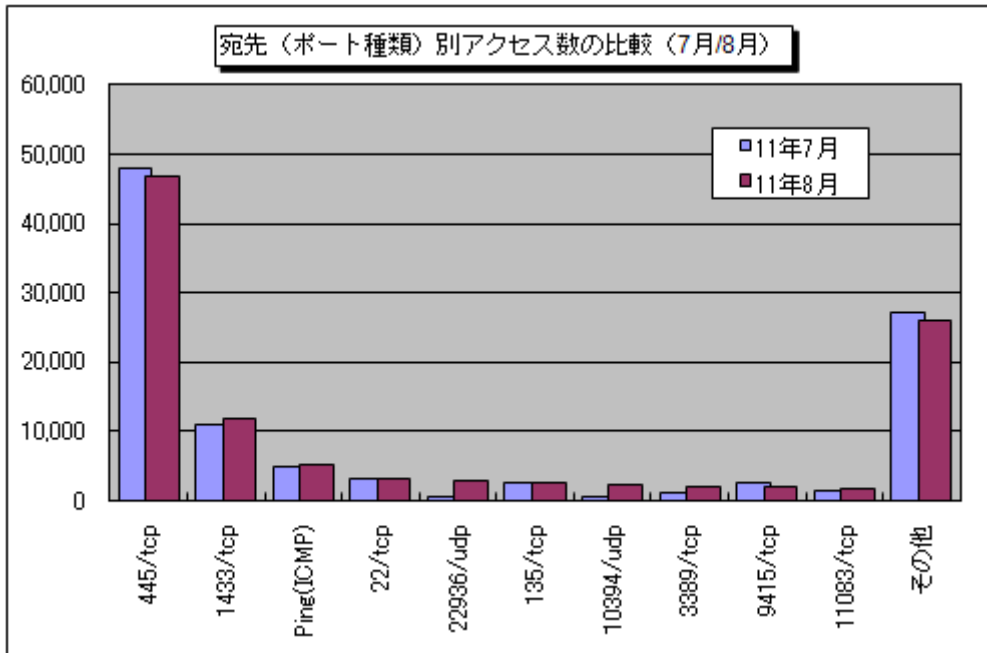
図 5-2：宛先（ポート種類）別アクセス数の比較（7 月/8 月）
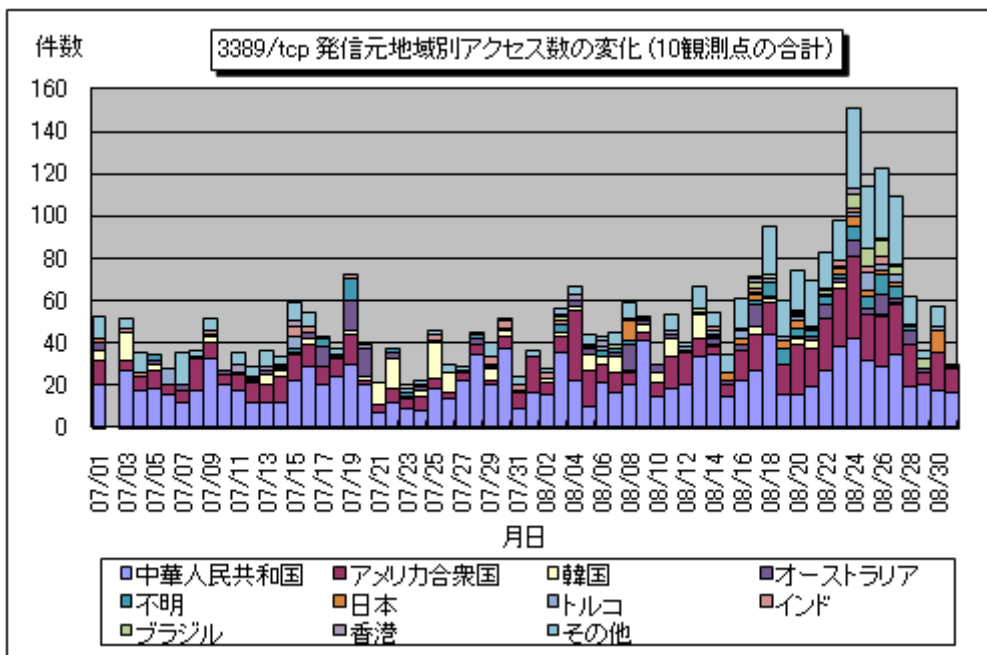
図 5-3：3389/tcp 発信元地域別アクセス数の変化（10 観測点の合計）

※7/2 は保守作業のため、システムを停止しています。

以上の情報に関して、詳細はこちらをご参照ください。

別紙 3_インターネット定点観測（TALOT2）での観測状況について

http://www.ipa.go.jp/security/txt/2011/documents/TALOT2-1108.pdf

『他機関・ベンダーの各種統計情報は以下のサイトで公開されています。』

一般社団法人 JPCERT コーディネーションセンター：http://www.jpcert.or.jp/

@police：http://www.cyberpolice.go.jp/

フィッシング対策協議会：http://www.antiphishing.jp/

株式会社シマンテック：http://www.symantec.com/ja/jp/

トレンドマイクロ株式会社：http://www.trendmicro.com/jp/

マカフィー株式会社：http://www.mcafee.com/japan/

株式会社カスペルスキー：http://www.viruslistjp.com/analysis/

■お問い合わせ先

IPA セキュリティセンター 加賀谷／宮本

Tel:03-5978-7591 Fax:03-5978-7518

E-mail isec-info@ipa.go.jp